(12) UK Patent Application (19) GB (11) 2 365 160 (13) A

(43) Date of A Publication 13.02.2002

(21) Application No 0028128.7

(22) Date of Filing 17.11.2000

(30) Priority Data
(31) 9928722 (32) 03.12.1999 (33) GB

(71) Applicant(s)
Security & Standards Limited
(Incorporated in the United Kingdom)
Suite A,192 Moulsham Street, Chelmsford, Essex, CM2 OLG, United Kingdom

(72) Inventor(s)
Nicholas Henry Pope
John Gordon Ross

(74) Agent and/or Address for Service
Williams, Powell & Associates
4 St Paul's Churchyard, LONDON, EC4M 8AY, United Kingdom

(51) INT CL[7]
G06F 1/00

(52) UK CL (Edition T)
G4A AAP

(56) Documents Cited
GB 2359156 A
GB 2337353 A
WO 98/40809 A2
WO 01/63878 A1
US 5958050 A
Computer Networks and ISDN systems Vol. 28 1996, (North Holland Publishing, Amsterdam) P Pays and F Comarmond, "An intermediate and payment system technology" pages 1197-1206

(58) Field of Search
UK CL (Edition S) G4A AAP
INT CL[7] G06F 1/00 , H04L 9/32
ONLINE: WPI, PAJ, EPODOC, INSPEC

(54) Abstract Title
Validation system for secure electronic commerce

(57) A validation system is provided for giving an indication of trustworthiness of a subject upon request from a user, including subject assessment means operable to obtain subject data from a data source, indicating means operable to provide to a user the results of the subject assessment, timing means operable to generate an indication of the time at which a request by a user is made, and receipt generating means operable to generate a receipt indicating at least one of the user, the subject assessment and the time of the request. The receipt can be used as evidence of an intended transaction with a subject. The system can also include recording means operable to record user requests and/or other user data relating to one or more subjects, and processing means operable to provide to a user an indication of the results of the subject assessment and/or recorded subject data.

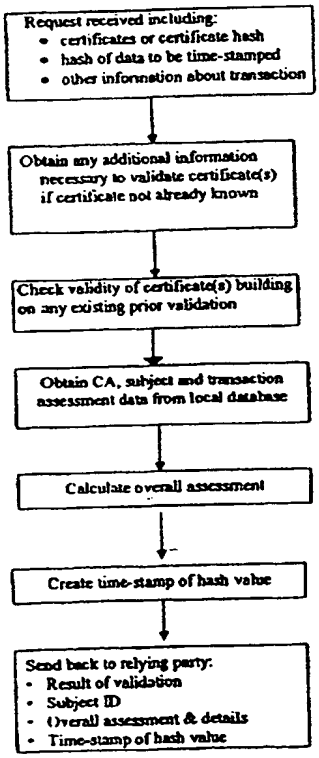

Figure 2

GB 2 365 160 A

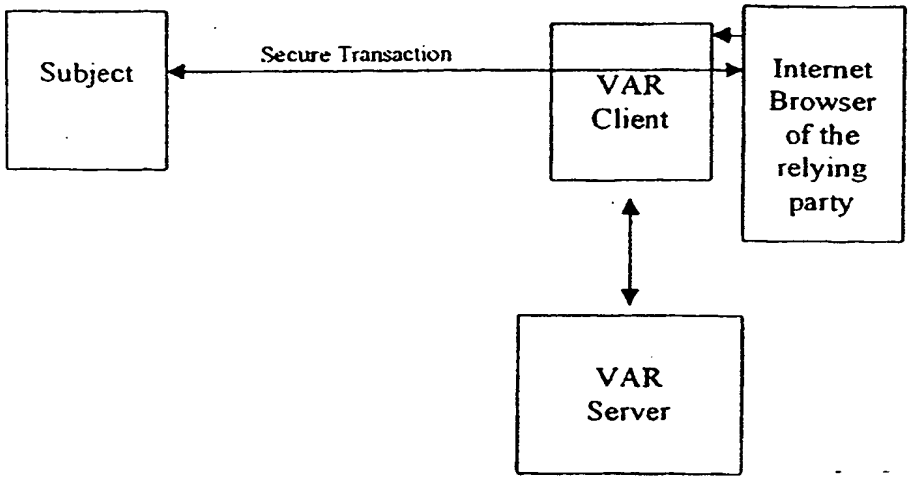
Subject
Secure Transaction
VAR Client
Internet Browser of the relying party
VAR Server

Figure 1

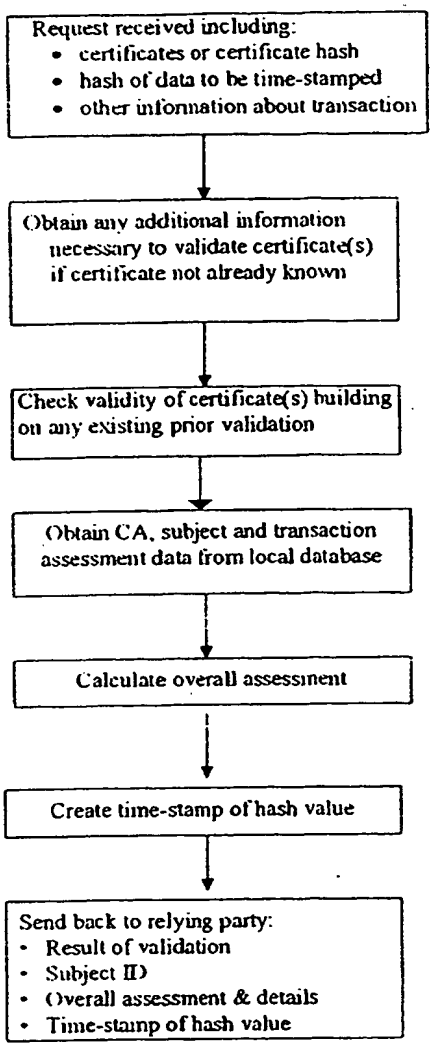
Request received including:
• certificates or certificate hash
• hash of data to be time-stamped
• other information about transaction
Obtain any additional information necessary to validate certificate(s) if certificate not already known
Check validity of certificate(s) building on any existing prior validation
Obtain CA, subject and transaction assessment data from local database
Calculate overall assessment
Create time-stamp of hash value
Send back to relying party:
• Result of validation
• Subject ID
• Overall assessment & details
• Time-stamp of hash value

Figure 2

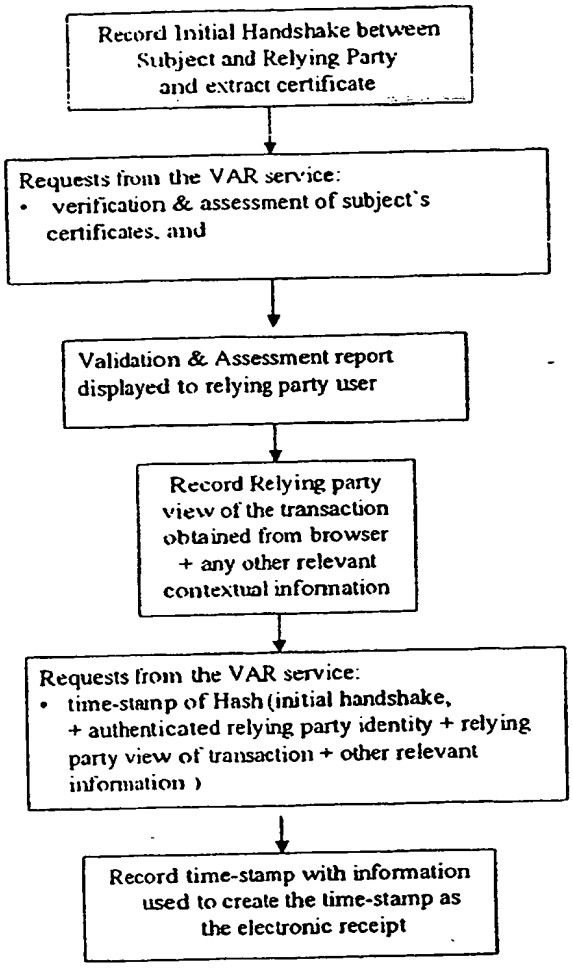
Record Initial Handshake between Subject and Relying Party and extract certificate
Requests from the VAR service:
• verification & assessment of subject's certificates, and
Validation & Assessment report displayed to relying party user
Record Relying party view of the transaction obtained from browser + any other relevant contextual information
Requests from the VAR service:
• time-stamp of Hash (initial handshake, + authenticated relying party identity + relying party view of transaction + other relevant information)
Record time-stamp with information used to create the time-stamp as the electronic receipt

Figure 3

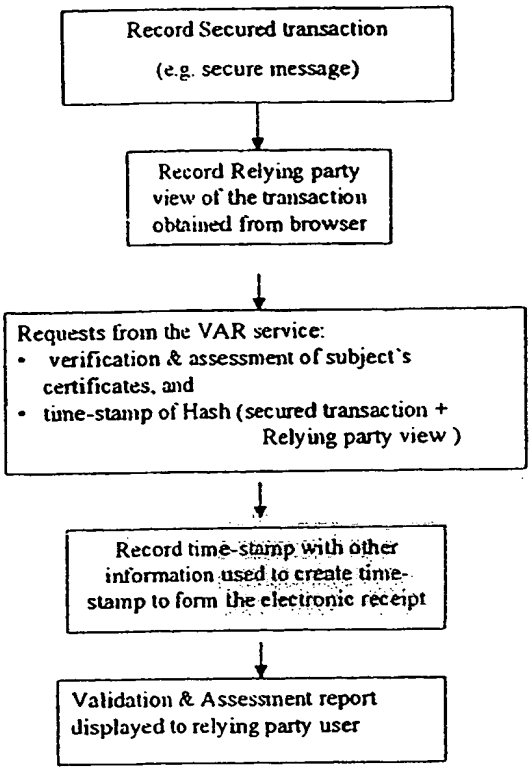
Record Secured transaction
(e.g. secure message)
Record Relying party view of the transaction obtained from browser
Requests from the VAR service:
• verification & assessment of subject's certificates, and
• time-stamp of Hash (secured transaction + Relying party view)
Record time-stamp with other information used to create time-stamp to form the electronic receipt
Validation & Assessment report displayed to relying party user

Figure 4

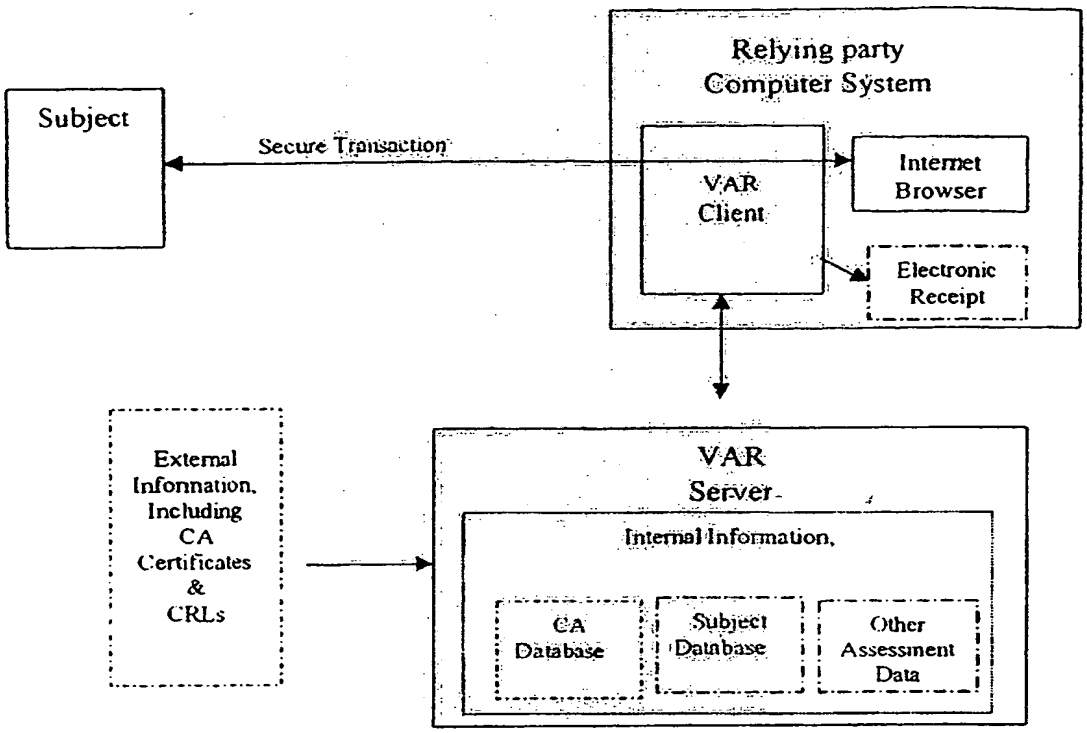
Relying party
Computer System
Subject
Secure Transaction
VAR
Client
Internet
Browser
Electronic
Receipt
External
Information,
Including
CA
Certificates
&
CRLs
VAR
Server
Internal Information,
CA
Database
Subject
Database
Other
Assessment
Data

Figure 5

5

VALIDATION SYSTEM FOR SECURE ELECTRONIC COMMERCE

The present invention relates to a validation system, including assessment and receipts (termed VAR), for use in electronic commerce performed, for example, over the Internet (World Wide Web).

Security protocols such as SSL (Secure Socket Layer, now standardised as Transport Layer Security (TLS) protocol), S/MIME (Secure MIME), SET (Secure Electronic Transactions) provide a means of securing e-commerce transactions and authenticating the trading partner. These security protocols make use of X.509 public key certificates as the basis for authenticating the remote party in an electronic commerce transaction either directly using digital signatures or indirectly using authenticated keys. X.509 public key certificates are obtainable from ITU-T X.509(93) Directory Authentication Framework, also published as International Standard ISO/IEC 9594-8.

Concerns relating to the validity of an identity authenticated using such protocols include the following:

a) the validity of the certificate has been compromised (e.g. due to the key being compromised). In such a situation the validity of the certificate needs to be revoked. X.509 defines a mechanism using a Certificate Revocation List to distribute a list of revoked certificates securely;

b) the certificate is used in situations for which is not intended (i.e. invalid use of certificates);

c) the certificate is fraudulent.

An Internet standard protocol has been defined for carrying out on-line checks on the validity of X.509 certificates (OCSP: On-line Certificate Status Protocol - Internet RFC2560). This protocol provides access to a service which can check the validity of the certificate, including whether it has been revoked.

It is becoming common for CAs to publish a statement of its certification practices, defining the policies and procedures used for operating its services. This information may be used to assess the trustworthiness of a CA and the hence the certificates it produces, however, this requires significant knowledge and expertise by the human user. Standard codes of practice and assessment criteria for certification authorities are being developed.

Such security protocols generally are designed to provide authentication at the time the transaction takes place. However, when the authentication is used to support electronic receipts the authentication information needs to remain valid over a long period so that the transaction information can be checked if there is a subsequent dispute over the transaction.

Thus a further concern is how to maintain the validity of authentication of a long period.

Two solutions are commonly used for this for X.509 digital signatures; one is for a trusted system to produced a signed time-stamp linked to fingerprint of the signed data. The other is to use a trusted archive supporting long term verification. A fingerprint is typically applied by a hash,

or message digest, algorithm to the signed data. Currently, no equivalent solution exists for SSL.

A third concern with the current system of e-commerce include:

a) the relying party has no means of assessing the trustworthiness of the e-commerce trading partner;

b) it is difficult for the normal relying party, to assess quickly whether certificates and other verification information have been issued and are being used in a trustworthy and legitimate manner. It can take a significant time to collect the relevant information and require expert knowledge to provide such an assessment.

The present invention seeks to provide an improved validation system.

According to an aspect of the present invention, there is provided a validation system for giving an indication of trustworthiness of a subject upon request from a user, including subject assessment means operable to obtain subject data from a data source, indicating means operable to provide to a user the results of the subject assessment, timing means operable to generate an indication of the time at which a request by a user is made, and receipt generating means operable to generate a receipt indicating at least one of the user, the subject assessment and the time of the request.

The receipt can be used as evidence of an intended transaction with a subject.

It is envisaged that the validation system may include transaction means operable to enable a transaction to be

performed between a user and a subject through the system or with verification of the transaction by the system, in which case the receipt generating means can generate a receipt indicating occurrence and, preferably, the details of, the transaction. With this embodiment, it is possible to provide independent evidence of the transaction. The term receipt used herein is intended to include evidence of a transaction that can be used by the relying party to support a claim that the transaction has taken place.

According to another aspect of the present invention, there is provided a validation system for giving an indication of trustworthiness of a subject upon request from a user, including subject assessment means operable to obtain subject data from at least one data source, recording means operable to record user requests and/or other user data relating to one or more subjects, and processing means operable to provide to a user an indication of the results of the subject assessment and/or recorded subject data.

This aspect can enable other data, such as previous validations of a subject and/or recommendations or problems with a subject to be considered in the assessment of a subject. Advantageously, the processing means is operable to generate a trustworthiness indicator based upon the assessed and/or stored data on a subject. The trustworthiness indicator can be generated on the basis of the type of assessment data and predetermined weighting factors. For example, some types of data such as insolvency or previous legal problems can be given high weighting factors while less important types of data, such as time of delivery can be given low weighting factors. Similarly, positive types of data can be given factors which in practice offset negative

data. Of course, some types of data, such as insolvency, can be set to cause a negative assessment of trustworthiness irrespective of other positive data. Of course, the features of the aspect described above can be combined together, as will be apparent from the specific description below.

The preferred embodiments provide a computerised system (with associated user software), which is accessible via a data network, which can provide one or more of the following services for secure electronic commerce (e-commerce):

a) check validity of information supporting the authenticity of an electronic commerce transaction, including public key certificates;
b) provide an assessment of the "trustworthiness" of a secured e-commerce transaction;
c) provide an electronic receipt as evidence of the transaction.

The preferred embodiment provides a validation system which can offer an integrated service which:

a) provides a check on the validity of certificates used for authentication;
b) provides a simple means for the user to assess the trustworthiness and previous trading record of the trading party, and the strength of the security used;
c) guides the user as whether he should proceed with the electronic trade or not;
d) provides the user with simple to understand information on the implications of a particular trade;
e) provides a means of collecting receipts which is

applicable to a range of security protocols including those which are not directly based on basic digital signatures as defined in X.509.

There is currently no recognised mechanism for providing long term evidence, for use as an electronic receipt, when trading using web based technology which integrates with existing web security protocols such as SSL. Furthermore, with current web technology that uses active web pages (that is, including software which create web page dependent on local characteristics) there is a degree of uncertainty with what the user may see not being determined exclusively from what was originally secured and received over the network. There is a need to include further contextual information, such as the web image as displayed on the web-viewer, to ensure that there is certainty that the receipts relates directly to what is perceived by web-user.

The term 'subject', is used herein to indicate the party in an e-commerce transaction which is the subject of validation and assessment by this system. The term 'relying party', is used herein to indicate the party in an e-commerce transaction which relies on the results of the validation and assessment. For example, in the case of trading over the Internet using Web protocols, the merchant may be the subject and the buyer may be the relying party. In the case of a signed electronic mail item the originator may be the subject and the recipient acting on the e-mail may be the relying party.

An embodiment of the present invention is described below, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a block diagram of an embodiment of system employing a VAR server;

Figure 2 is a flow chart of an embodiment of operation of the system of Figure 1;

Figure 3 is a flow chart of an embodiment of validation operation;

Figure 4 is a flow chart of an embodiment of validation operation using S/MIME; and

Figure 5 shows in more detail an embodiment of system.

The preferred embodiment includes the following features:

1) the VAR Client, software resident in the relying parties system, which monitors the secure transaction between the relying party's Internet browser and a subject,

2) a networked VAR Server used by the relying party to provide validation and assessment services as well as a time-stamp used in creating an electronic receipt.

The VAR Server is a computerised system, which can be accessibly via a data network such as the public Internet or a private Intranet. The server is used by a party relying on certificates to support secured electronic commerce transaction (e.g. purchase of goods or services from an Internet web server) to help check and assess the security of the transaction. The VAR Server may be composed of several networked computers that together provide the VAR services. The VAR Server, its relationship to the relying party and a

secured transaction with a remote subject is illustrated in Figure 1.

The VAR Server:

a) determines the validity of the electronic security information, including certificates, on which an e-commerce transaction relies;

b) provides an assessment of the trustworthiness of the transaction based on:

i) information about the CA such as whether the CA meets recognised criteria (e.g. as defined in EU legislation, standardised or accepted codes of practice);

ii) information about the subject such as checks carried out by the CA when registering the subject, the amount of trading already carried out with the subject (derived from any record of previous validation check done on that subject), any reports of problems from subscribers, or is a recognised to be a member of an identified scheme for payments or codes of practice;

iii) information about the transaction such as legal context and cryptographic algorithms employed;

c) provides a time-stamp of the transaction which can be used by the relying party to produce an electronic receipt of the transaction.

The relying party uses the VAR Server:

a) to validate and get an assessment of a transaction's security;

b) to time-stamp the transaction information.

During the transaction the VAR client records both the secured data transferred during the transaction, or security tokens containing the security significant parts the transaction (e.g. initial SSL handshake), as well as the relying parties view of that transaction (e.g. as displayed), the identity of the relying party and other relevant contextual information. The secured data and the contextual information are time-stamped. The VAR Server may check the authenticity of the relying party's identity before applying the time-stamp. The relying party stores the secured transaction or tokens and the contextual information, along with the time-stamp, as the electronic receipt or passes the receipt to the VAR Server for storage on behalf of the user.

The relying party view is used as the relying party's claim for the transaction. If the subject disputes this claim it can replay the transaction from the secured transaction.

This embodiment may be used to support a range of protocols for securing the transaction (e.g. SSL / SMIME / SET / Signed code). More specifically, in use, the relying party sends to the VAR Server, relevant information (see below) for validation, assessment of the secured transactions with the subject, and to request a time-stamp as the basis of an electronic receipt. This includes:

a) the subject's certificate (or chain of certificates) being relied upon for the security of the transaction, or if the certificate is already known to the VAR server a simplified representation (e.g. hash) of the certificate that can be used a key on the certificate related information in the subject database;

b) the cipher suite (identifier for the set of cryptographic algorithms and key lengths used to secure an SSL session) or algorithms used;

c) an indication of the current usage being validated and assessed (e.g. SSL server authentication, e-mail authentication);

d) the legal context (e.g. country) in which the relying party operates;

e) a hash (fingerprint) of the data to be time-stamped.

On reception of this information the VAR Server:

a) obtains any additional information (e.g. CA certificates, CRLs) needed to validate the received certificate (where possible arrangements will be made with CAs to provide a copy of the latest CRL information direct to the validation service and to inform the validation service of any updates);

b) checks the technical validity of the certificates) as required under X.509, including full certificate path and revocation checks;

Note: if the subject's certificate is already known to the VAR service validation checks can be carried out beforehand and the result held in the subject database. Only checks on certificate validity period need be repeated at time of request from the relying party;

c) the VAR Server obtains from a local database of known CAs information on the all the CA's business standing and certification practices on which the e-commerce transaction relies including:

i) identification of recognised codes of practice/assessment criteria to which the CA conforms, (e.g. requirements of certification service providers

issuing of Qualified Certificates in Annex II of the Draft European Directive on Electronic Signatures), or other information on the standing of the CA;

ii) information on the Limit of liability of CA;

iii) legal system under which CA operates;

iv) registration procedures of CA including any checks on the business standing of the certified subjects;

v) limits on the usage by subjects of the certificates (e.g. SSL server only, S/MIME authentication only, only given legal contexts).

(Of course, the above list can be altered or amplified with other criteria.)

d) the VAR Server looks up in its database for information on the subject of the validation and assessment including:

i) the length of time over which the server has been trading (i.e. the time that validation checks were first made on that subject),

ii) the number of validation checks that had been made over a recent period (e.g. 1 month),

iii) the number and gravity of any reported problems when trading with the subject,

iv) legal system under which the subject operates, whether the server conforms to recognised codes of practice (e.g. the Interactive Media in Retail Group code of practice for electronic commerce), and other information on the standing of the identified entity.

v) whether the subject is a recognised merchant under a payment system (e.g. credit card)

vi) whether the subject is a member a scheme which has recognised codes of practice for e-commerce

vii) other locally held information about the Subject.

(Note: Initially, no information may be available for a subject. The latter items of data may only be collected for subjects which are major e-commerce traders.)

e) the VAR Server looks up in its other database for other assessment information relating to the transaction:

i) any specific legal requirements or constraints that may exist;

ii) a rating of the security of given cryptographic algorithms and key lengths or cipher suites,

iii) any independent rating of the subject's commercial and security practices such as can be established through accredited membership of a recognised code of practice

f) the VAR Server provides an overall assessment of the transaction in simple terms covering:

i) any limits of liability associated with certificates (e.g. as indicated in the CA's practices or explicitly given in the certificate). In cases where the validation depends on several certificates, the lowest value is chosen;

ii) abstract assessment for the level of trust in the certified subject and the security of the transaction based on the features of the transaction including:

- the number of problems reported with the subject divided by the number of transactions,

- the subject's commercial and security practices
- the registration procedures of the subject's CA,
- conformance of each CA to recognised codes of practice,
- the cryptographic algorithms, including key lengths used to protect the transaction;

iii) the legal framework with which certificates comply & under which server operates (as indicated in the CA's practice or explicitly given in the certificate). In the case where the validation depends on several certificates issued under different legal frameworks, if no equivalence or cross recognition is known to exist between the legal systems then no common legal framework is identified.

For each of these features individual assessment values are assigned. First, minimum assessment value of all the features are found. Then, the individual assessments are combined mathematically in one or more ways. The minimum value of all the combinations and the individual assessments is then used to provide the overall assessment.

The validation service creates a time-stamp by signing a hashed value concatenated with the current time.

On completion of the above steps, the validation service sends back in a response to the relying party:

a) an indication of whether the technical validation checks are passed;

b) the identity of the certificate subject;

c) the time-stamp;

d) information giving reasons for any failure of checks;

e) output of overall assessment;

f) details in the certificates;

g) other used in the assessment such as the country of registration, legal and tax implication, previous track record;

h) information held on the CA and subject including information used as input to the overall assessment process.

The validation service maintains a record of the request and response related to the subject for use in later assessments of the subject.

Figure 2 illustrates the sequence of actions carried out by the VAR Server.

The above description is for a service offering validation, assessment and time-stamping in a single operation. The VAR Server can also be used to provide a time-stamping service as a separate independent operation without validation and assessment. Similarly validation and assessment can be provided without time-stamping.

The exchanges between the VAR client and the server are protected path using SSL, a cryptographic message check code or other security mechanisms which at least authenticates the server and protects the integrity of the exchange. There is no requirement for the identification of the relying party for the VAR service to operate, although this may necessary

for the purposes of charging and controlling use of the VAR service. Also, authentication of the relying party at their request could be offered as an optional extension to the time-stamping service to authenticate an identifier of the relying party which could be included in the time-stamp.

The VAR Server provides an accessible web page where any problems with the use of services provided by a given certified subject can be reported. A problem report is e-mailed back to the person reporting the problem who is requested to reply confirming the source and verity of the problem report. Once confirmed the problem report is added to the local database entry for that Subject.

VAR Client Details

The VAR Client monitors the communications between the subject and the relying party's secured Internet browser application (e.g. Internet web browser or Internet e-mail reader). From this information:

a) It identifies in the protocol where certificates, and other security relevant information such as algorithm identifiers, exist and uses these to obtain a validation and assessment from the VAR Server.

b) It records all the secured transaction, or electronic tokens containing the security significant parts of the transaction (e.g. initial SSL handshake), which is to be recorded for use as part of the electronic receipt.

The VAR Client also obtains information from the Internet browser giving the relying party's view of the transaction. This relying party view can include one or more of:

- a snap shot image of the display at the key points in the transaction,
- structured data resulting from decrypting the secured transaction,
- a résumé of the transaction as needed for financial accounts,
- the transaction session key encrypted using a key encrypting key known only to the relying party.
- the identity of the relying party which is authenticated by the VAR Server before creating the time-stamp.

In order to create an electronic receipt the VAR client calculates the hash of the secured transaction and the relying party view of the transaction, to be time-stamped by the VAR Server. The secured transaction, the relying party view of the transaction and time-stamp are then placed in long-term storage medium (e.g. floppy disk, write only CD) to form the electronic receipt, or passed to the VAR Server for storage on behalf of the relying party. The relying party view can be used as it's claim of what went on in the transaction. If there is a dispute with the relying party's claim of the electronic receipt based on the relying party view, then the subject can be required to replay the transaction from the secured transaction data.

The time-stamp gives independent proof that the transaction occurred at a given time.

The VAR client can either request a validation and assessment of a secured transaction on its own, a time-stamp on its own

or a combination of validation and assessment with time-stamp.

In the case of a secured interactive transaction (e.g. using SSL), the relying party requests a validation & assessment and a time-stamp after the initial handshake which establishes the security of the transaction. The time-stamp provides basic evidence of the existence of the transaction. The results of the validation and assessment can be displayed to the user for him/her to get an assessment and make an informed decision before proceeding with the rest of the transaction (e.g. revealing credit card numbers to the subject and proceeding with the order). In order to produce a full electronic receipt the relying party may also request an additional time-stamp of all the secured transaction, with the relying party view, when the transaction is complete.

The assessment may be presented and displayed to the user in various ways depending on the uses needs. It can be simplified to a three states displayed to the user in the form of traffic lights:

Red indicating that there is significant risk in trading with this site and so it is recommended that the site be avoided;

Amber indicating that there is some risk when trading with this site and so it is recommended that the site should be used with caution. Additional information and guidance is available for the user to make an informed decision on whether to proceed with the trade or not;

Green indicating that there is minimal risk associated with using this site.

Alternatively, the user can be presented with a five star assessment report. A user can request the display of full details of the assessment report should he want more information, such as the country of registration, legal and tax implication, previous track record, etc.

In the case of a secured e-mail or other non-interactive secured transaction, the message can be forwarded to the VAR Client when a message is selected for processing by the user. The relying party requests the validation and assessment, and a time-stamp of the whole message from the server as in a single operation.

This embodiment also identifies an extension to SSL to provide a signature of the all the secured transaction from the subject to strengthen the evidential value of records kept by the relying party. This proposed extension to the SSL protocol is to allow the relying party to request that the combined hash of data passing in each direction is digitally signed by the remote SSL party (i.e. the SSL server). This signature can be used by the relying party with the rest of the transaction to provide proof of the transaction.

The sequence of operations for using the validation service with an interactive security protocols, such as SSL, is illustrated in Figure 3.

In the case of security protocols there is no initial handshake (S.MIME/SET/Signed code), the validation and assessment is requested at the same time as the time-stamp for the secured transaction plus the relying party view. The

sequence of operations for using the validation service with S/MIME is illustrated in Figure 4.

The structure of a possible implementation of this invention (which includes the VAR Client and the VAR Server), is illustrated in Figure 5.

The above description is for transactions using X.509 based digital signatures or using X.509 certificates to provide authenticated keys as in SSL. The system can also be applied to other forms of certificates including the variant of X.509 defined in PGP (RFC 1991, RFC 2440) or EDIFACT certificates. The system can also apply to other security protocols using digital signature (e.g. Microsoft Authenticode, sign JAR files, signed XML) in a similar way as for secure e-mail.

Similar services may also be used for SET.

The main advantages of the described embodiments over existing validation and time-stamping systems include the ability:

a) to provide an overall assessment of the security transaction in terms which:

i) avoids the need for detailed technical knowledge and understanding of all the complexities of the security mechanisms used,

ii) incorporates the range of factors which effect the security of the transaction including trustworthiness of the CA, subject and protections applied to the transaction,

iii) provides the assessment in simple terms combining a range of complex factors into a simple rating,

b) to provide an electronic receipt of a secured electronic transaction in a way which is:

i) applicable across a range of security protocols including the secured web access protocol SSL,

ii) avoids the VAR system having to handle any sensitive, private or personal encryption keys,

iii) provides evidence of what the user saw linked to the secured transaction,

c) to provide an integrated validation, assessment and time-stamping service supporting the relying party;

d) does not require changes to the user's secure application (Internet Browser) software;

e) does not require changes to the subjects' secure application software (WEB server).

CLAIMS

1. A validation system for giving an indication of trustworthiness of a subject upon request from a user, including subject assessment means operable to obtain subject data from a data source, indicating means operable to provide to a user the results of the subject assessment, timing means operable to generate an indication of the time at which a request by a user is made, and receipt generating means operable to generate a receipt indicating at least one of the user, the subject assessment and the time of the request.

2. A system according to claim 1, including transaction means operable to enable a transaction to be performed between a user and a subject through the system or with verification of the transaction by the system.

3. A system according to claim 2, wherein the receipt generating means is operable to generate a receipt indicating occurrence and/or details of the transaction.

4. A system according to claim 1, 2 or 3, including recording means operable to record user requests and/or user data relating to one or more subjects.

5. A system according to any preceding claim, including means for recording the amount of transactions performed by a user for retrieval by the indicating means.

6. A system according to any preceding claim, including storage means operable to store receipts generated by the generating means.

7. A system according to any preceding claim, including means operable to access user data from remote data services.

8. A system according to any preceding claim, wherein the indicating means is operable to clarify a subject into a plurality of trustworthy and not trustworthy categories.

9. A validation system for giving an indication of trustworthiness of a subject upon request from a user, including subject assessment means operable to obtain subject data from at least one data source, recording means operable to record user requests and/or other user data relating to one or more subjects, and processing means operable to provide to a user an indication of the results of the subject assessment and/or recorded subject data.

10. A system according to claim 9, wherein the processing means is operable to generate a trustworthiness indicator based upon the assessed and/or stored data on a subject.

11. A system according to claim 10, wherein the trustworthiness indicator is generated on the basis of the type of assessment data and predetermined weighting factors.

12. A validation system substantially as hereinbefore described with reference to and as illustrated in the accompanying drawings.

Amendments to the claims have been filed as follows

CLAIMS

1. A validation system for giving an indication of trustworthiness of a subject upon request from a user, including means for obtaining subject data from a data source, validation means for validating subject data obtained from the data source, assessment means operable on the basis of pre-selected criteria to assess the subject from the obtained subject data and the validation of said data, and indicating means operable to provide to a user the results of the subject assessment.

2. A validation system according to claim 1, wherein the validation means is operable to validate obtained subject data from a third party source or from a database of the system.

3. A validation system according to claim 2, wherein the subject data is a trading certificate and the validation means is operable to access a database of an authority issuing said trading certificate or from said database.

4. A validation system according to any preceding claim, wherein the validation means includes security determining means operable to determine the security of communication between a subject and a user, the assessment means being operable to assess the subject from the determined security, the obtained subject data and the validation of said data.

5. A validation system according to any preceding claim, including level determining means operable to categorise the result of the assessment into one of a predetermined number

of levels, said determined level being indicated by the indicating means.

6. A system according to any preceding claim, including transaction means operable to enable a transaction to be performed between a user and a subject through the system or with verification of the transaction by the system.

7. A system according to claim 7, including receipt generating means operable to generate a receipt indicating occurrence and/or details of a transaction.

8. A system according to claim 7, including storage means operable to store receipts generated by the receipt generating means.

9. A transaction monitoring system for monitoring a transaction between a subject and a user located remote from one another, which transaction is carried out over a communication link between the subject and the user; the system including monitoring means operable to monitor events occurring during a transaction, clock means and recording means operable to record at least one said event and a time stamp indicative of time provided by the clock means.

10. A system according to claim 9, including transaction means operable to enable a user to communicate with a subject to perform a transaction, the transaction means being coupled to the monitoring means.

11. A system according to claim 9 or 10, wherein the communication link is the Internet.

12. A system according to claim 11, wherein the recording means is operable to record web pages as viewed by a user, said web page views representing said transaction events.

13. A validation system substantially as hereinbefore described with reference to and as illustrated in the accompanying drawings.

Application No:	GB 0028128.7	**Examiner:**	Michael Powell Waters
Claims searched:	1 to 12	**Date of search:**	21 November 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G4A (AAP)

Int Cl (Ed.7): G06F (1/00) H04L (9/32)

Other: Online: WPI, EPODOC, PAJ, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X, E	GB 2359156 A	(REUTERS) figures 2 and 4 and pages 9 to 14 for example	1,2,9,10 and 11
X	GB 2337353 A	(IBM) for example see page 6 lines 17 to 30, page 12 line 45	1 to 6 and 9
X, E	WO 01/63878 A1	(TRADE-SAFELY.COM) see figures 2b and 4	1
X	WO 98/40809 A2	(CHA!) figures 2,3 and 4C especially	1 to 11
X	US 5958050	(GRIFFIN et al) column 6 lines 52 to 62 and figures 3 and 5	9 to 11
X	Computer Networks and ISDN systems Vol. 28 1996, (North Holland Publishing, Amsterdam) P Pays and F Comarmond, "An intermediate and payment system technology", pages 1197-1206, especially paragraph 3.1		1 to 11

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.